PASSWORD POLICY

Title:	Password Policy
Abstract:	This document establishes the Company's Password Policy and outlines the requirements for creating and protecting passwords. The policy is mandatory.
Author:	*[Author Name]*
Business Approval:	*[Approver Name]*
Date Issued:	*[Date Issued]*

AMENDMENT RECORD

Issue Number	Date Issued	Description and Author
001		Original Issue

Company Password Policy

Policy Statement

This document establishes the Company's Password Policy and outlines the requirements for creating and protecting passwords.

Passwords are the entry point to company resources. Creating strong passwords and protecting access is essential in ensuring that the network, hardware and software remains secure. All personnel, business partners and personnel affiliated with third parties who have access to the company resources are responsible for taking the appropriate steps, as outlined below, to create and protect their passwords.

All the requirements stated herein must be met if technically available on the operating system (OS) platform.

Definitions

This policy covers the creation and protection of passwords and as such the following definitions apply:

• **Password**: A password is a sequence of characters used to determine that a computer user requesting access to a computer system is really that particular user. It is one-half of a typical set of credentials used in authentication. The other half is the User ID.

• **User ID**: a username establishes the identity of the user. The user ID is generally visible when entered at a keyboard or other input device.

Passwords are generally used in combination with some form of identification, such as a username or account number. While a username (user ID) establishes the identity of the user for the computer or system, the password, which is known only to the authorized user, authenticates that the user is who he or she claims to be. This means that the basic function of passwords is to prove to the system or network that you are who you say you are.

Objectives

This policy outlines the rules for:

- The creation and protection of strong passwords.
- The frequency of changing those passwords, as well as other requirements.
- The roles and responsibilities for password management within the company.

Compliance

Compliance with this policy is required of all personnel and of all business partners and personnel affiliated with third parties who have access to the company network, hardware and software. Any employee found to have violated this policy shall be deemed to have violated their Employee Conduct Agreement. Business partners and personnel affiliated with third parties who violate this policy are subject to temporary or permanent removal from company facilities, removal of access to the network and to any company computing device, and the relevant disciplinary actions as stipulated in their business contract.

Requirements

Weak or non-compliant passwords are a major vulnerability in any computing system, and are the most commonly exploited security feature. Insufficient password security on one account can expose the entire

company network (and possibly a substantial portion our customers data and email) to malicious activities.

To protect the company network, a strong password must be used. Strong passwords contain a combination of alphabetic characters plus symbols and numbers. Once generated, the users and system administrators must also protect these passwords by not sharing them with anyone else. As such, all passwords shall be created and protected, where technically possible, in accordance with the requirements stated below.

Password Creation and Management

All company passwords (e.g., email, web, desktop computer, etc.) used on company systems shall be "strong" passwords with the following characteristics:

- A minimum password length of eight (8) characters.
- Contain at least two (2) alpha characters (a-z, A-Z).
- Contain at least one (1) Upper Case Alpha character (A-Z).
- Contain at least one (1) numeric character (0-9).
- Contain at least one (1) "special" character, such as the following:
  ~ ` ! @ # $ % ^ & * ( ) _ - + = , . / \ { } [ ] ; : < > ? " '
- The maximum number of consecutive failed login attempts shall be set to 5. The system shall be disabled after that for at least five (5) minutes. After three sets of up to five (5) failed login attempts, the system shall be disabled and require administrator intervention and password reset.
- Be changed every one hundred eighty (180) days for general users.
- Be changed every sixty (60) days for users with "high level" system privileges, e.g. system, application, database or network administrators.
- Not be reused until after four (4) other different passwords have been selected
- A minimum of ninety (90) days shall elapse before reuse of a password is permitted
- Not be a dictionary word in any language or slang, dialect, jargon, etc.
- Not be based on personal information, e.g., name of family member, date of birth, driver license number, etc.
- Not be any form of dates (dates are part of most crack algorithms).
- Not contain a 3/4-letter word (e.g., dogs.99, 23.leaf etc., these password types are split and can be cracked faster).
- Not contain a 3/4 letter/word reciprocity (e.g., He1ght# =Height#, L00K!89 =LOOK!89, etc).
- Not contain inappropriate language.
- Not contain consecutive numbers (1234), letters (ABCD) or keyboard strokes (QWERTY).
- Password expiry warning set to fifteen (15) days.
- User accounts shall be locked after one hundred eighty (180) consecutive days of inactivity.
- Third party accounts shall be locked after ninety (90) consecutive days of inactivity.

- Administrator accounts shall be locked after thirty (30) consecutive days of inactivity.
- Blank or default vendor/software passwords shall be changed prior to deployment.
- Account passwords shall be changed on initial login.
- A secure hardware mechanism for storing passwords may be used or issued. This must be encrypted and approved by the company. Hardware such as a USB key running KeePass or similar security software is likely to be approved.

Password Protection

Passwords must be protected in accordance with the following requirements:

• Do not use the same password for company accounts as for other non-company accounts (e.g. Facebook, Twitter, Instagram etc.).

• Use different passwords for different accounts, systems, and applications.

• Do not share company passwords with anyone, including administrative assistants or secretaries. All passwords shall be treated as sensitive, company information.

• Do not reveal a password over the phone to anyone or reveal a password in an email message. System Administration or Help Desk calls/emails are exempt but must follow the provisions below.

• Do not talk about a password in front of others.

• Do not reveal a password to co-workers while on vacation.

• Do not use the "Remember Password" feature of applications (e.g., Web browsers, Outlook etc.).

• Do not write passwords down and store them anywhere in your office unless absolutely necessary. Precautions shall be taken to protect passwords that are written down, i.e., must be stored in a **locked** safe, file cabinet, or desk.

• Do not store or transfer passwords in a file on any computer system (including PDAs or similar devices) without encryption.

• If an account or password is suspected to have been compromised, report the incident and change all passwords immediately.

• Password cracking or guessing may be performed on a periodic or random basis by the company or its delegates. If a password is guessed or cracked during the scans, the user will be required to immediately change it. If not changed in two (2) business days the user account will be disabled.

• A password history of no more than five (5) shall be maintained (where supported).

Additional Password Protections

The following additional requirements apply:

- Personal Computers (PCs) shall always use a screen saver with a strong password.
- Software shall provide for the non-display or blotting of passwords on any display screen. In addition, the software must provide the capability of encrypting passwords and automatically forcing password change activity, where possible.
- All applications, processes, data feeds/transactions, etc. shall enforce authentication, where possible.

- Help-desk support personnel will have primary responsibility for resetting user passwords initiated through a helpdesk call or personal contact with the user. No password shall be reset without positively verifying the identity of the user. As a minimum, at least two items of user personal data, e.g., employee ID number, mother's maiden name, date of birth, place of birth, etc., shall be used for verification purposes for each password reset. If fewer than two items of personal data are available, new passwords may not be provided over the telephone, but must be emailed to the employee at the email address on record. The user shall be notified via email whenever their password has been changed or reset.

Roles and Responsibilities

It is the responsibility of all company personnel, business partners and personnel affiliated with third parties who have access to the network, to ensure that compliance with this policy is maintained at all times.

HR Manager

- Distribute this Password policy throughout the company including new employees and contractors.
- Write any associated network security documents as required.
- Develop, maintain, and update the company internal network security documents.
- Approve and track all policy exceptions.
- Ensure all network security documents are readily accessible to all employees.

Employees and Users

- Understand and observe the password security requirements and controls specified by this policy and appropriate supporting security documents.
- Properly use, protect, and dispose of company sensitive data, including passwords in accordance with this policy and other applicable security policies.
- Follow the requirements specified herein for proper creation and protection of passwords.

System Administrators, SuperUsers and Network Managers

- Are responsible for the initial assignment of a user's password. Users shall be instructed to change passwords at their discretion and/or change them at system prompts per the requirements stated. User generated or system generated passwords shall be randomly selected, not obvious, not associated with the user in any way (e.g. badge number, name, etc.), not easily guessed, or shared with others.
- No password may be reset without verifying the identity of the user (see above for verification method).
- Passwords must be removed or changed immediately when an individual leaves the employ of the company, when an individual is suspended from duty, or whenever they no longer have need to access the company network.
- System administrators shall follow the requirements above for all servers and network devices they access/administer.
- Ensure remotely accessible services on the network require authentication.
- Ensure authentication processes over the network are encrypted.
- Ensure all default community passwords are changed.
- Provide technical support.

Key Terms

Authentication is the process of determining whether someone is, in fact, who he or she is declared to be. Authentication is commonly done through the use of logon passwords. Knowledge of the password is assumed to guarantee that the user is authentic.

Business Partners Includes, but is not limited to, contractors, subcontractors, team members, alliance members, and consultants.

Company Network The company's internal network where company personnel, or an authority designated by management, controls all routing and security,

Password Aging Password aging is a technique used by system administrators to defend against bad passwords within an organization. Password aging means that after a set amount of time, usually 180 days, the user will be prompted to come up with a new password.

Password Cracking While passwords are a vital component of system security, they can be cracked or broken relatively easily. Password cracking is the process of figuring out or breaking passwords in order to gain unauthorized entrance to a system or account. It is much easier than most users would think. (The difference between cracking and hacking is that codes are cracked, machines are hacked.) Passwords can be cracked in a variety of different ways. The simplest is the use of a word list or dictionary program to break the password by brute force.

User Individuals provided with authorized access to information and information systems managed by the company.